Hewlett Packard Enterprise

Building Security Use Cases with ArcSight ESM Content H7G90S

Building Security Use Cases with ArcSight ESM provides you with detailed knowledge of the ArcSight security problem solving methodology, within the ESM context. In this course, you learn the methodologies to develop use cases for current business scenarios, derived from the top business drivers in the market.

Building Security Use Cases with ArcSight ESM Content	
Price	USD $2,400
Links to local schedules, pricing and registration	**US/Canada** **Mexico/Latin America** **Brazil**
HP course #	H7G90S
Category	Security
Duration	3 days

Audience

This advanced course is intended for those whose primary responsibilities include:
- Defining organization's security objectives
- Building ArcSight ESM content to adhere to those objectives

Prerequisites

To be successful in this course, you must have:
- Common network device functions, such as routers, switches, hubs, etc.
- TCP/IP functions, such as CIDR blocks, subnets, addressing, communications, etc.
- Windows operating system tasks, such as installations, services, sharing, navigation, etc.
- SIEM terminology, such as threat, vulnerability, risk, asset, exposure, safeguards, etc.
- Security directives, such as Confidentiality, Integrity, Availability
- Basic understanding of TCP/IP networking and database concepts
- Enterprise security experience [highly advantageous]

Course objectives

At the end of this course, you will be able to:
- In an ArcSight ESM context, define Use Case
- Using the Use Case worksheet from an initial problem statement, generate requirement statements and prioritize objectives
- Identify data sources and ESM resources required to fulfill the objectives of the use case
- Create identified ESM content
- Construct ArcSight Active Channels to provide advanced analysis of the event stream
- Develop ArcSight Rules to allow correlation activities
- Build event-based data monitors to provide real-time viewing of event traffic
- Package formulated ESM content for Use Case into ArcSight Resource Bundle

Course outline

Understanding Use Cases
- Defining Use Cases
- Building ArcSight Use Cases
- ArcSight Best Practice Considerations

Delivering ArcSight Use Cases
- Activity 1 - Solution Delivery Using Packages
- Activity 2 – Using the ArcSight Use Case Resource

Compliance Use Cases – Self Study
- Use Case 1 – FISMA
- Use Case 2 – PCI
- Use Case 3 - SOX

Appendix
- Module 1 and Module 3 Topic Quizzes

Implementing Custom ArcSight Solutions
- Internal Threats and Perimeter Threats

Internal Threats
- Use Case 1 - Privileged Account Usage
- Use Case 2 - Network Logon Status
- Use Case 3 - Account Deletion Policy
- Use Case 4 – Removable Media Policy

Perimeter Threats
- Use Case 5A - Zero Day Attack Policy
- Use Case 5B - Zero Day Attack Policy Confirmation
- Use Case 6 – Reducing False Positives Policy
- Use Case 7 -Anti-Virus Metrics
- Use Case 8 - Disallowed Services Monitoring
- Use Case 9 - Custom Use Case

Additional Use Case Drivers
- Additional Use Case Drivers

Learn more at

hpe.com/us/training/security

H7G90S Ver A.00

c04723039 June 2015

Hewlett Packard Enterprise